

APPLICATION FOR UNITED STATES LETTERS PATENT

ON INVENTION FOR:

INTERNET SYSTEM

BY INVENTOR: Gorkem I. Ates

Agt. Doc. No.: ATEG21A

RICHARD L. MILLER

REGISTERED PATENT AGENT

12 PARKSIDE DRIVE

DIX HILLS, NEW YORK 11746-4879

PHONE: (516) 499-4343

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN that I, Gorkem I. Ates,

a citizen of TURKEY and resident of:

Tandogan, Ankara, Turkey

have invented certain new and useful improvements in a(n):

INTERNET SYSTEM

of which the following is a full, clear, concise and exact
description:

1 Inventor: Gorkem I. Ates

2 Invention: INTERNET SYSTEM

3 DOC. No.: ATEG21A

4 DISK NAME: SPEC002A,2B,C

5 BACKGROUND OF THE INVENTION

6 Field of the Invention:

7 The present invention relates to a system. More
8 particularly, the present invention relates to an Internet
9 system.

10 Description of the Prior Art:

11 Many business and scientific organizations in the United
12 States which use more than one computer in their operations
13 couple the computers together through a network.

14 The network permits the computers to be islands of
15 processing which may share resources or data through
16 communication over the network. The data which may be
17 communicated over the network may take the form of programs
18 developed on a user's computer, data file created on a user's
19 computer, electronic mail messages, and other data messages and
20 files which may be generated or modified by a user at a user's
21 computer.

1 Typically, the user's computer includes an operating system
2 for controlling the resources of the user's computer, including
3 its central processing unit ("CPU"), memory (both volatile and
4 non-volatile memory), and computer peripherals such as printers,
5 modems, and other known computer peripheral devices. The user
6 typically executes application programs and system services to
7 generate data files or programs.

8 Most computers are coupled to a network through a network
9 communications printed circuit card which is typically resident
10 within each computer system. This communications card typically
11 includes processors, programs, and memory to provide the
12 electrical signals for transmission of data and implement the
13 protocol which standardizes the messages transmitted through a
14 network.

15 To communicate data from a user's application program or
16 operating system service, a protocol stack is typically
17 implemented between the communication card for the network and
18 the operating system services and application programs. The
19 typical protocol stack used on most open networks is a Transport
20 Control Protocol/Internet Protocol ("TCP/IP").

21 The TCP/IP stack includes a transport layer which divides a
22 data stream from an application program or service into segments
23 and which adds a header with a sequence number for each segment.

24 The TCP segments generated by the transport layer creates a
25 packet having a packet header and a data portion. The data
26 portion contains the TCP segment and the packet header contains a

0940121-09299
662260-12270460

1 source address identifying the computer sending a message and a
2 destination address identifying the computer for which the
3 message is intended. The IP layer also determines the physical
4 address of the destination computer or an intermediate computer,
5 in some cases, which is intended to receive the transmitted
6 message.

7 The packet and the physical addresses are passed to a
8 datalink layer. The datalink layer typically is part of the
9 program implemented by a processor on the communication card and
10 it encapsulates the packet from the IP layer in a datalink frame
11 which is then transmitted by the hardware of the communication
12 card. This datalink frame is typically called a packet.

13 At the destination computer, the communication card
14 implements the electrical specification of a hardware
15 communication standard, such as Ethernet, and captures a data
16 message from a source computer, with the word "message"
17 henceforth including the data entities packet and datalink frame.
18 The datalink layer at the destination computer discards the
19 datalink header and passes the encapsulated packet to the IP
20 layer at the destination computer.

21 The IP layer at the destination computer verifies that the
22 packet was properly transmitted, usually by verifying a checksum
23 for the packet. The IP layer then passes the encapsulated TCP
24 segment to the transport layer at the destination computer. The
25 transport layer verifies the checksum of the TCP message segment
26 and the sequence number for the TCP packet. If the checksum and

1 TCP sequence number are correct, data from the segment is passed
2 to an application program or service at the destination computer.

3 Modern information networks, e.g. the Internet, use servers
4 to store documents. In the World Wide Web (web), these documents
5 are addressed by uniform resource locators (URLs). URLs specify
6 the protocol by a prefix in the URL, such as http:// for Hyper
7 Text Transfer Protocol, the host in the Internet where the
8 document is stored, and the address of the document within the
9 host. The Web is thus not a single protocol, but a combination
10 of several protocols united by a common addressing scheme, i.e.
11 the URL.

12 The tremendous continuing growth of the Web makes it
13 necessary to have intermediate servers which perform caching
14 (store documents locally, such that the documents may be quickly
15 accessed from the local file system, instead of being
16 retransferred again from the original server. Such servers (see,
17 for example A. Luotonen, K. Atlis, World Wide Web Proxies,
18 Proceedings of First International World-Wide-Web Conference,
19 Geneva 1994) are referred to as caching proxy servers, or proxies
20 for short. See, also A. Chakhuntod, P. Danzig, C. Neerdaels, M.
21 Schwartz, K. Worrell, A Hierarchical Internet Object Cache,
22 USENIX 1996 ANNUAL TECHNICAL CONFERENCE, [http://usenix.org/](http://usenix.org/publications/library/proceedings/sd96/danzig.html)
23 [publications/library/proceedings/sd96/danzig.html](http://usenix.org/publications/library/proceedings/sd96/danzig.html)). Proxies
24 reduce network load, and shorten response times to the user.

1 The operation of a prior art proxy server 10 can best be
2 seen in figure 1, and as such, will be discussed with reference
3 thereto.

4 When a client 12 requests a new document from the proxy
5 server 10, the proxy server 10 copies the document from the
6 origin server 14 to its local file system in addition to sending
7 the document to the client 12. When another requests comes for
8 the same document, the proxy server 10 returns the document from
9 the cache 16, if the cached copy is still up to date. If the
10 proxy server 10 determines that the document may be out of date,
11 it performs an up-to-date check from the remote origin server 14
12 and refreshes the document, if necessary, before sending it to
13 the client 12.

14 Numerous innovations for network related systems have been
15 provided in the prior art that will be described. Even though
16 these innovations may be suitable for the specific individual
17 purposes to which they address, however, they differ from the
18 present invention.

19 A FIRST EXAMPLE, U.S. Patent No. 5,463,735 to Pascucci et
20 al. teaches a network system having a wide variety of
21 applications and particularly applicable to facilities management
22 systems that includes network controllers which continuously
23 process data related to building and industrial, environmental,
24 security and other automated system controls. Each network
25 controller has a network address indicative of a communication
26 link to which the network controller is connected, a local

04401224-09299
662260-2210460

1 address and a node drop ID to determine whether the network
2 controller is a configured or non-configured device. Data stored
3 in an archive device is downloaded to a destination network
4 controller in the absence of a routing table in the destination
5 network controller by transmitting a download request message
6 from the archive device to an intermediate network controller
7 with a routing table. The intermediate network controller
8 assumes control of the download request by transmitting the
9 message to the destination controller. The destination
10 controller acknowledges receipt of the message by transmitting an
11 acknowledge message back to the intermediate network controller,
12 which passes the acknowledge message to the archive device in
13 accordance with the routing information stored in the
14 intermediate network controller. Thus, as certain network
15 controllers are connected, disconnected or disabled during the
16 operation of the network, the control of a process is not
17 interrupted. Additionally, the network controllers are not
18 configured to store large amounts of routing data because a path
19 to a device can be established through other controllers with
20 routing information.

21 A SECOND EXAMPLE, U.S. Patent No. 5,727,159 to Kikinis
22 teaches a system wherein relatively low-end-computers, such as
23 portable, battery-powered computers ordinarily incapable of
24 Internet browsing functions may be used to browse the Internet.
25 The enhanced computing ability for such portables is provided by
26 a unique arrangement having a Proxy-Server with adequate

04401221-09229
652260-1221046

1 computing power for all World Wide Web (WWW) browsing and
2 downloading functions, and further capable of transposing
3 downloaded files to alternative, low-information-density form
4 suitable for rapid processing and display by connected portable
5 and other low-end computers. In some embodiments the data link
6 from the connected low-end units is a TCP/IP pipe, supporting
7 TCP/IP protocol, but not the many sophisticated extensions
8 usually associated with TCP/IP. In embodiments wherein battery-
9 powered units are used, connected to the Proxy-Server, battery
10 life is exhibited far beyond what would be expected for a
11 battery-powered computer with computing power for browsing the
12 Internet directly.

13 A THIRD EXAMPLE, U.S. Patent No. 5,754,857 to Gadol teaches
14 a system and method for automating workflow by distributing the
15 tasks required for the execution of said workflow over servers
16 and clients connected on a network. The disclosed system and
17 method allow the stages of the workflow to be performed
18 asynchronously, meaning that, once a workflow initiated by a user
19 has been initiated by a database server, the stages of the
20 workflow can be executed on respective network clients without
21 further interaction with the server (i.e. without requiring a
22 stateful connection between the clients and servers). This is
23 accomplished through the use of a workflow courier that embodies
24 all programs (encompassing rules governing the execution of the
25 workflow) and forms needed by clients to complete stages of the
26 workflow. The workflow courier also stores workflow state

1 information that indicates which stages of the workflow have been
2 completed. The executable programs are written in the platform-
3 independent Java programming language and are therefore
4 executable on any computer that has an installed Java browser.
5 After each stage is executed, the client executing that stage
6 updates the workflow courier and transmits the updated workflow
7 courier to a client having an associated user who is authorized
8 to perform the next step in the workflow. The updated state
9 information indicates to the recipient of the workflow which
10 stages remain to be completed.

11 A FOURTH EXAMPLE, U.S. Patent No. 5,862,344 to Hart teaches
12 apparatus and methods for providing processing system network
13 connectivity, and more particularly, for routing data packets
14 between at least two processing system networks. A first memory
15 for storing at least one address for each of the networks, and a
16 second memory for storing selectively at least one address for
17 particular ones of the networks, are provided. A control circuit
18 for routing a received data packet from a source network to a
19 destination network is also provided. The control circuit
20 utilizes a destination address which was retrieved from one of
21 the first memory and the second memory, in response to a
22 determination as to whether at least one address corresponding to
23 the destination network is stored in the second memory.

24 A FIFTH EXAMPLE, U.S. Patent No. 5,864,852 to Loutonen
25 teaches a proxy server, wherein variable length URLs are digested
26 and thereby homogenized, such that each URL is converted to a URL

1 fingerprint that has a unique identity and a same fixed size.
2 The URL fingerprint is used to map the URL to a proxy server
3 cache directory structure. A unique file name may also be
4 generated from the URL fingerprint for each URL. The same bits
5 are used in the file name, such that any given file can be
6 remapped later to a directory structure that had been expanded or
7 collapsed, so that the first bits are not unique to a particular
8 hierarchy. A unique cache information file is included in the
9 directory to store document-related information for each other
10 file in the directory for quick access. Accordingly, the
11 invention provides an addressing and cache organization scheme
12 that allows quick access to documents that contain all the
13 relevant information for each of the URLs.

14 A SIXTH EXAMPLE, U.S. Patent No. 5,892,903 to Klaus teaches
15 a system and method for detecting security vulnerabilities in a
16 computer network. The system includes an IP spoofing attack
17 detector, a stealth port service map generator, a source port
18 verifier, source routing verifier, an RPC service detector and a
19 Socks configuration verifier. Each of these verifiers make be
20 operated separately or as a group to detect security
21 vulnerabilities on a network. Each verifier may be programmed to
22 exhaustively test all ports of all computers on a network to
23 detect susceptibility to IP spoofing attacks, access to services
24 with little or no authorization checks or misconfigured routers
25 or Socks servers. The detected vulnerabilities or the location
26 of services having little or no authorization checks may be

1 stored in a table for reference by a network administrator. The
2 service map generated by the stealth service map generator may be
3 used to identify all service ports on a network to facilitate the
4 operation of the other verifiers which send service command
5 messages to service ports to detect their accessibility. A
6 graphic user interface (GUI) may be used to provide input and
7 control by a user to the security verifiers and to present
8 options and display information to the user.

9 A SEVENTH EXAMPLE, U.S. Patent No. 5,913,040 to Rakavy et
10 al. teaches methods and apparatus for selecting advertisements
11 and other information from a computer network database based on
12 user defined preferences and transmitting the selected
13 advertisement in background mode over a communications link
14 between the computer network and a local computer with minimal
15 interference with other processes communicating over the
16 communications link. This method includes monitoring the
17 communications link and transmitting portions of the
18 advertisement when the communications link line utilization is
19 below a preestablished threshold. Methods and apparatus are also
20 provided for displaying or otherwise presenting the selected
21 advertisements on the user's computer. Additional methods and
22 apparatus are provided for selecting and presenting information
23 stored on a local storage media based on user defined
24 preferences.

25 It is apparent that numerous innovations for network related
26 systems have been provided in the prior art that are adapted to

1 be used. Furthermore, even though these innovations may be
2 suitable for the specific individual purposes to which they
3 address, however, they would not be suitable for the purposes of
4 the present invention as heretofore described.

0940331-0999
0940331-0999

1

2

3

4

5

6

7

8

1 denial of service attacks, because their IP addresses are not
2 revealed to clients and thus hackers.

3 BRIEFLY STATED, YET STILL ANOTHER OBJECT of the present
4 invention is to provide an Internet system. The system includes
5 a main server and at least one participant server. The main
6 server stores information to be requested over the Internet by a
7 client so as to form a request for information and has an IP
8 address. The at least one participant server has an IP address
9 and electrically communicates with the main server. The at least
10 one participant server does not receive the request for
11 information from the client, but rather the main server receives
12 the request for information over the Internet from the client and
13 requests over the Internet that the at least one participant
14 server send the requested information over the Internet back to
15 the client. If the at least one participant server does not have
16 the requested information, the requested information is
17 downloaded from the main server to the at least one participant
18 server. When the at least one participant server sends the
19 requested information over the Internet back to the client, the
20 at least one participant server assigns to the requested
21 information the IP address of the main server and not the IP
22 address of the at least one participant server.

23 The novel features which are considered characteristic of
24 the present invention are set forth in the appended claims. The
25 invention itself, however, both as to its construction and its
26 method of operation, together with additional objects and

1 advantages thereof, will be best understood from the following
2 description of the specific embodiments when read and understood
3 in connection with the accompanying drawing.

0940460 "TELEPHONE"

1

2

3

4

5

6

7

8

LIST OF REFERENCE NUMERALS UTILIZED IN THE DRAWING

Prior Art

10 prior art proxy server
12 client
14 origin server
16 cache

Present Invention

20 Internet system of the present invention
22 main server for storing information 24 to be requested over
Internet 26 by client 28 so as to form a request for
information 30
24 information to be requested over Internet 26 by client 28 so
as to form a request for information 30
26 Internet
28 client
30 request for information
32 IP address of main server 22
34 at least one participant server
36 IP address of at least one participant server 34
38 IP address of client 28
40 at least one nearest participant server of at least one
participant server 34

1 DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

2 Referring now to the figures, in which like numerals
3 indicate like parts, and particularly to figure 2, the Internet
4 system of the present invention is shown generally at 20.

5 The Internet system 20 comprises a main server 22 for
6 storing information 24 to be requested over the Internet 26 by a
7 client 28 so as to form a request for information 30 and having
8 an IP address 32.

9 The Internet system 20 further comprises at least one
10 participant server 34 having an IP address 36 and electrically
11 communicating with the main server 22.

12 The at least one participant server 34 does not receive the
13 request for information 30 from the client 28, but rather the
14 main server 22 receives the request for information 30 over the
15 Internet 26 from the client 28 and requests over the Internet 26
16 that the at least one participant server 34 send the requested
17 information 30 over the Internet 26 back to the client 28, and if
18 the at least one participant server 34 does not have the
19 requested information 30, the requested information 30 is
20 downloaded from the main server 22 to the at least one
21 participant server 34.

22 When the at least one participant server 34 sends the
23 requested information 24 over the Internet 26 back to the client
24 28, the at least one participant server 34 assigns to the
25 requested information 24 the IP address 32 of the main server 22

1 and not the IP address 36 of the at least one participant server
2 34.

3 The main server 22 is a TCP/IP server that assigns jobs to
4 the at least one participant server 34 dynamically without
5 relocating the client 28 using neither HTTP nor HTML commands so
6 as to take relocating process away from top networking OSI layers
7 to 3rd level of Internet working OSI that is IP so as to enable
8 starting downloading of the requested information 24 from one of
9 the at least one participant servers 34 and finishing the
10 downloading from another of the at least one participant server
11 34 without ever noticing server alteration.

12 The top networking OSI layers are at least one of TCP, HTTP,
13 and application level.

14 The method for using the Internet system 20 can best be seen
15 in figures 3A-3D, and as such, will be discussed with reference
16 thereto.

17 STEP 1: Make the request for information 30, over the Internet
18 26, by the client 28, to the main server 22 and not to
19 the at least one participant server 34; making the
20 request for information 30 to the at least one
21 participant server 34 the normal behavior of today's
22 networking equipment and software.

23 STEP 2: Examine an IP address 38 of the client 28, by the main
24 server 22.

1 STEP 3: Seek the nearest at least one participant server 34, by
2 the main server 22, so as to form an at least one
3 nearest participant server 40.

4 STEP 4: Request over the Internet 26, by the main server 22
5 acting like an orchestra leader, that the at least one
6 nearest participant server 40 send the requested
7 information 24 to the client 28, packet-by-packet, over
8 the Internet 26.

9 STEP 5: Determine if the at least one nearest participant
10 server 40 has the requested information 24.

11 STEP 6: Label, by the at least one nearest participant server
12 40, each packet with the IP address 32 of the main
13 server 22, which enables the client 28 which has a port
14 open only for main server addresses to accept said
15 packets, if answer to STEP 5 is yes.

16 STEP 7: Send the requested information 24 with the IP address
17 32 of the main server 22, by the at least one nearest
18 participant server 40, to the client 28, over the
19 Internet 26.

20 STEP 8: Download the requested information 24 from the main
21 server 22 to the at least one nearest participant
22 server 40, which will distribute the load of the main
23 server 22 to the at least one nearest participant
24 server 40 when lacking multicasting so as to save
25 costs, by virtue of the at least one nearest
26 participant server 40 being relatively easy and

inexpensive to add as compared to clustering more servers to the main server 22, if answer to STEP 5 is no.

STEP 9: Return to STEP 6.

The step of making the request for information 30, over the Internet 26, by the client 28, to the main server 22 includes making the request for at least one of a streaming video and an audio, over the Internet 26, by the client 28, to the main server 22.

The step of seeking the nearest at least one participant server 34, by the main server 22, so as to form an at least one nearest participant server 40 includes seeking the nearest at least one participant server 34, by the main server 22, so as to form the at least one nearest participant server 40 that has the most bandwidth and CPU and other serving requirements needed to furnish the requested information 24 to the client 28.

It will be understood that each of the elements described above, or two or more together, may also find a useful application in other types of constructions differing from the types described above.

While the invention has been illustrated and described as embodied in an Internet system, however, it is not limited to the details shown, since it will be understood that various omissions, modifications, substitutions and changes in the forms and details of the device illustrated and its operation can be

652260 "FETTER"

made by those skilled in the art without departing in any way from the spirit of the present invention.

Without further analysis, the foregoing will so fully reveal the gist of the present invention that others can, by applying current knowledge, readily adapt it for various applications without omitting features that, from the standpoint of prior art, fairly constitute characteristics of the generic or specific aspects of this invention.

09401 Feb 19 1964